Shifting Into EMV:

An Insider's Guide

Thursday, October 8th

Elavon

Agenda

- ✓ EMV Overview
- ✓ The Importance of a Layered Security Approach
- ✓ EMV Certification Levels
- ✓ EMV Readiness Checklist
- ✓ Pros and Cons of Fully-Integrated, Stand-Alone and Semi-Integrated Solutions
- ✓ Q&A

60 minute presentation with questions throughout

Email presentations@elavon.com for a copy of the presentation. A link to the recording will also be sent in the days following the event.

Elavon

Payment Security Panel

Michael LaCross
Market Development & Innovation
22 years of experience in electronic payments

Jay Forthman
Head of Services & Retail
20+ years as a leader in professional services and solution engineering

Susan Rue
Security Domain Expert
20+ years experience in security payment solution implementations

Wendy Zickus
EMV Product & Innovation
20 + years experience in payment card architecture and design

Elavon

Security Threat

Security Threats

The Threats impact every business!

Elavon

Security in Retail

Percentage of data breaches affecting the Retail industry

Source: Trustwave Global Security Report

A typical PMS or POS may contain millions of customer data records

Source: Krebs On Security – May 2014

Personal Identifiable Information (PII) is worth 10x that of credit card data on the black market

Source: Networkworld – Feb 2015

Elavon

Security in Retail

Compared to the all-industry average, the retail sector experienced more incidents involving denial of service and point-of-sale intrusions.

Incidents by pattern: All industries versus retail.

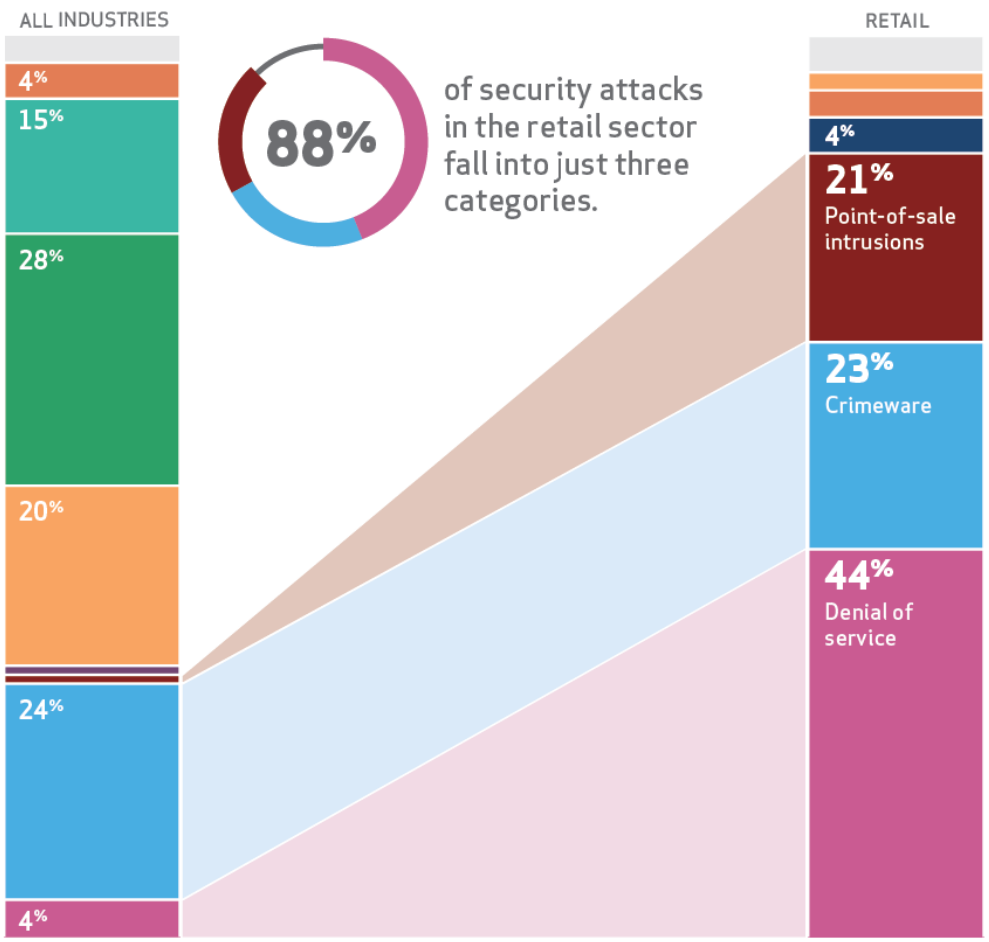


FIGURE 1
INCIDENTS BY PATTERN: ALL INDUSTRIES VERSUS RETAIL

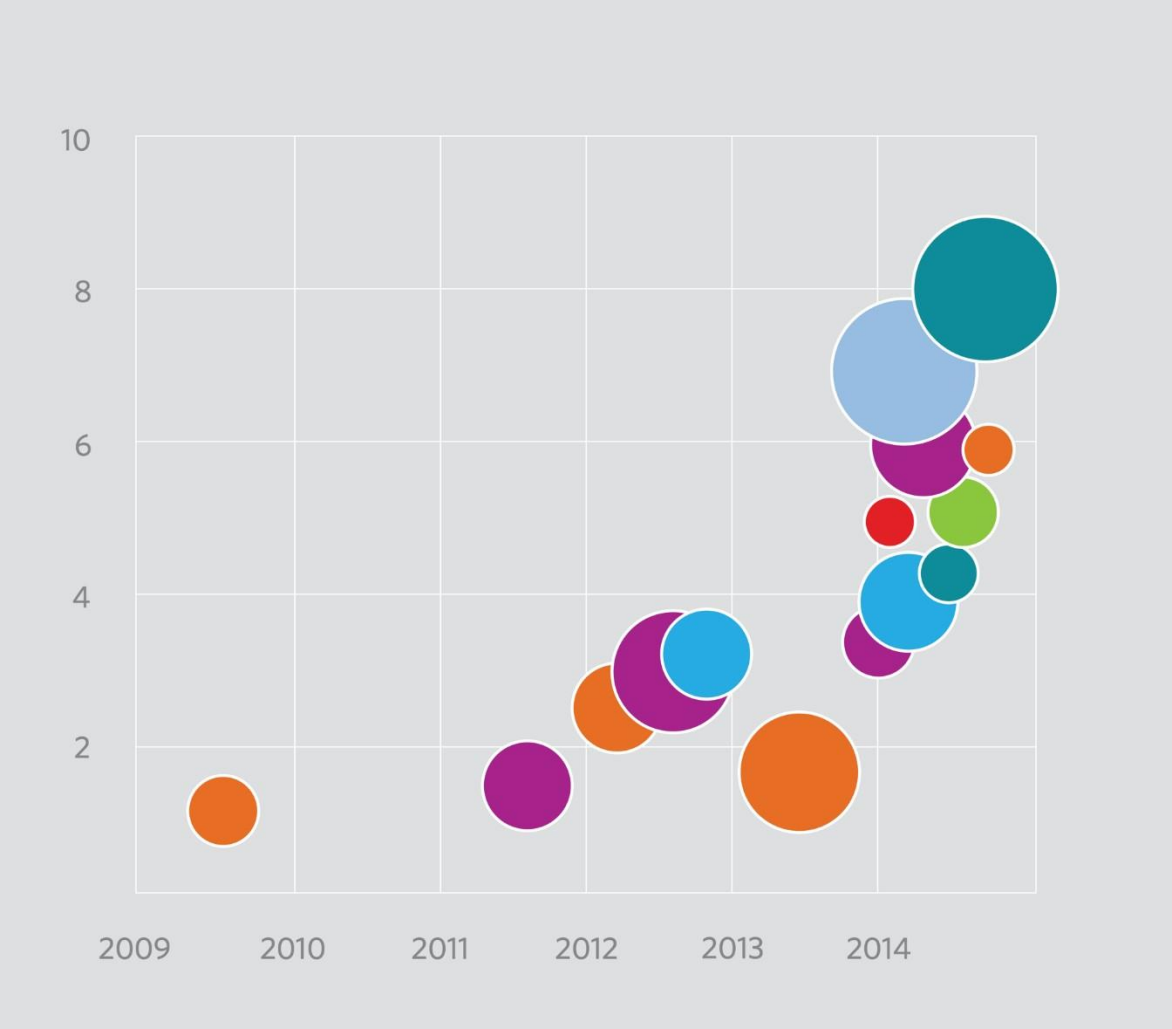
Almost 90% of security incidents in the retail sector involved denial of service attacks, crimeware, or point-of-sale intrusions. Attackers were often able to compromise systems and walk away with data in days or less. But in over 50% of cases it took retail organizations months or more to discover a breach had occurred.

verizon

2015 Data Breach Investigations Report
RETAIL

Elavon

Trending Malware



Bubbles represent various malware instances, such as Lusy POS, Soraya, JackPOS, New POSThings, etc.

Source: http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-evolution-of-point-of-sale-pos-malware

Elavon

Definition

$52,000 - $87,000

Forecasted average loss for a breach of 1,000 records

Source: Verizon 2015 Data Breach Investigation Report

Elavon

EMV Impacts All Verticals

Transactions that Occur in a Card-Present Environment

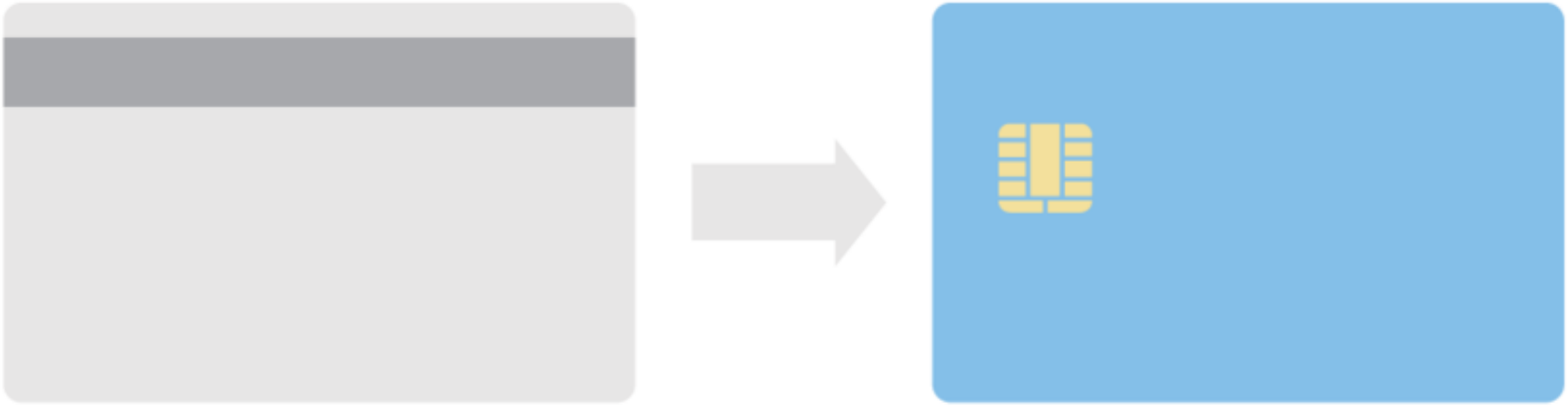
- Office of the Tax Collector – counter payments
- Licensing – Fishing, Pet, Beach
- DMV Offices – License, Registration Fees, Permit
- ABC Liquor Store
- Fan/Gear Shops
- Cafeteria
- Lodging Venues
- Tuition Counter Payments
- Hotel Gift Shops/Restaurants/Bars

Elavon

EMV LIABILITY: WHAT IT MEANS

Elavon

What is EMV?



“Europay, MasterCard, and Visa.”

Translation: Credit cards will be equipped with a computer chip that’s extremely hard to counterfeit.

What Does EMV Liability Shift Mean?

Merchants hold liability for EMV counterfeit cards[1]

Only applies to card present EMV-enabled cards

Brands have different rules for PCI relief

Merchants hold liability for lost or stolen cards that they accept for payment

[1]Effective October 1, 2015

Elavon

Why Now?

Elavon

When?

How Does This Impact My Business?

INTERLINK Cirrus AFFN STAR pulse Credit Union 24 NYCE Maestro

Elavon

How Will This Impact Cardholders?

New Cards

Cards Stay in Terminal Longer

More Security

Contactless/Mobile

Elavon

Worldwide EMV Deployment and Adoption

Figures reported in Q4 2013 and represent the latest statistics from American Express, Discover, JCB, MasterCard, UnionPay and Visa, as reported by their member institutions globally.

Region	EMV Cards	Adoption Rate	EMV Terminals	Adoption Rate
Western Europe	794M	81.6%	12.2M	99.9%
Canada, Latin America and the Caribbean	471M	54.2%	7.1M	84.7%
Africa and Middle East	77M	38.9%	699K	86.3%
Eastern Europe	84M	24.4%	1.4M	91.2%
Asia Pacific	942M	17.4%	15.6M	71.7%

Region	EMV Cards	Adoption Rate	EMV Terminals	Adoption Rate
United States [estimates]	~17-20M	~1-2%	~2M	~20%

Source: Estimates stated from The Smart Card Alliance/EMV Migration Forum, May 2014

EMV and Card Present Fraud in UK and Canada

67%: % Losses fallen since 2004

58%: % Lost and stolen card fraud fell between 2004 – 2009

91%: Mail non-receipt fraud fallen since 2004

UK Cards Association

$142M to $38.5M CAD: Losses from debit card skimming fell between 2009-2012

Record Low: Interac debit card fraud losses fell to $29.5 million in 2013

Interac Association

$700 Million: Annual savings from counterfeit fraud prevention could total this much

EMV Adoption & its Impact on Fraud Management Worldwide
Mercator, January 2014

source: EMV Connection

Elavon

EMV: True vs. False

- Prevents **counterfeit fraud** at POS
- Protect against **counterfeiting cards**
- Create a different POS experience
- Store cardholder **data on a chip**
- Require a **new card**
- See **growing adoption** in the U.S. in the next 12-18 months

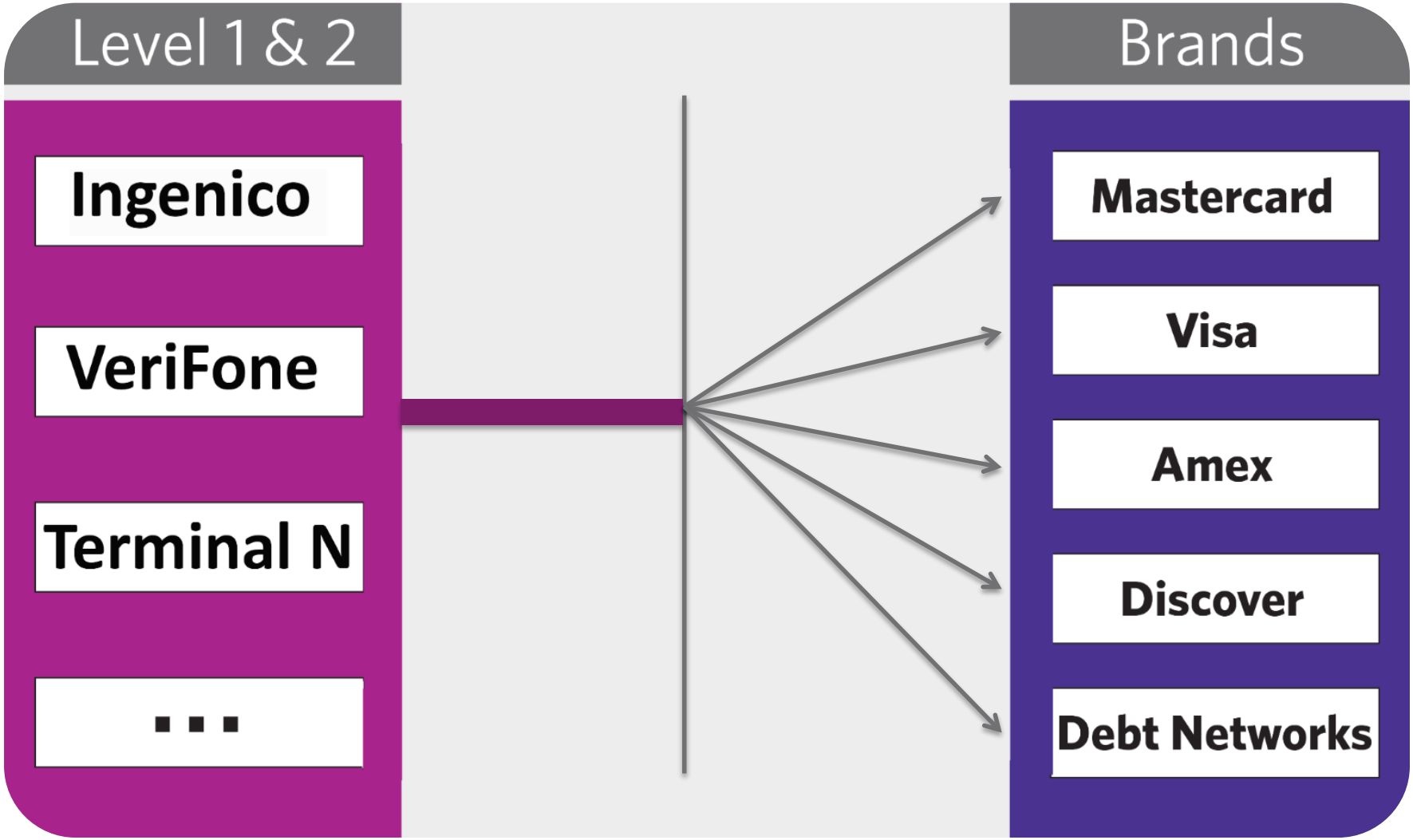
- Protect against **card-not-present fraud**
- Prevent **data breaches**
- Always require a **PIN**
- Be vulnerable to **wireless interception** of data
- Eliminate the need for **magnetic stripe**
- Be **universally adopted** in the U.S. for 3-4 years

EMV CERTIFICATION LEVELS

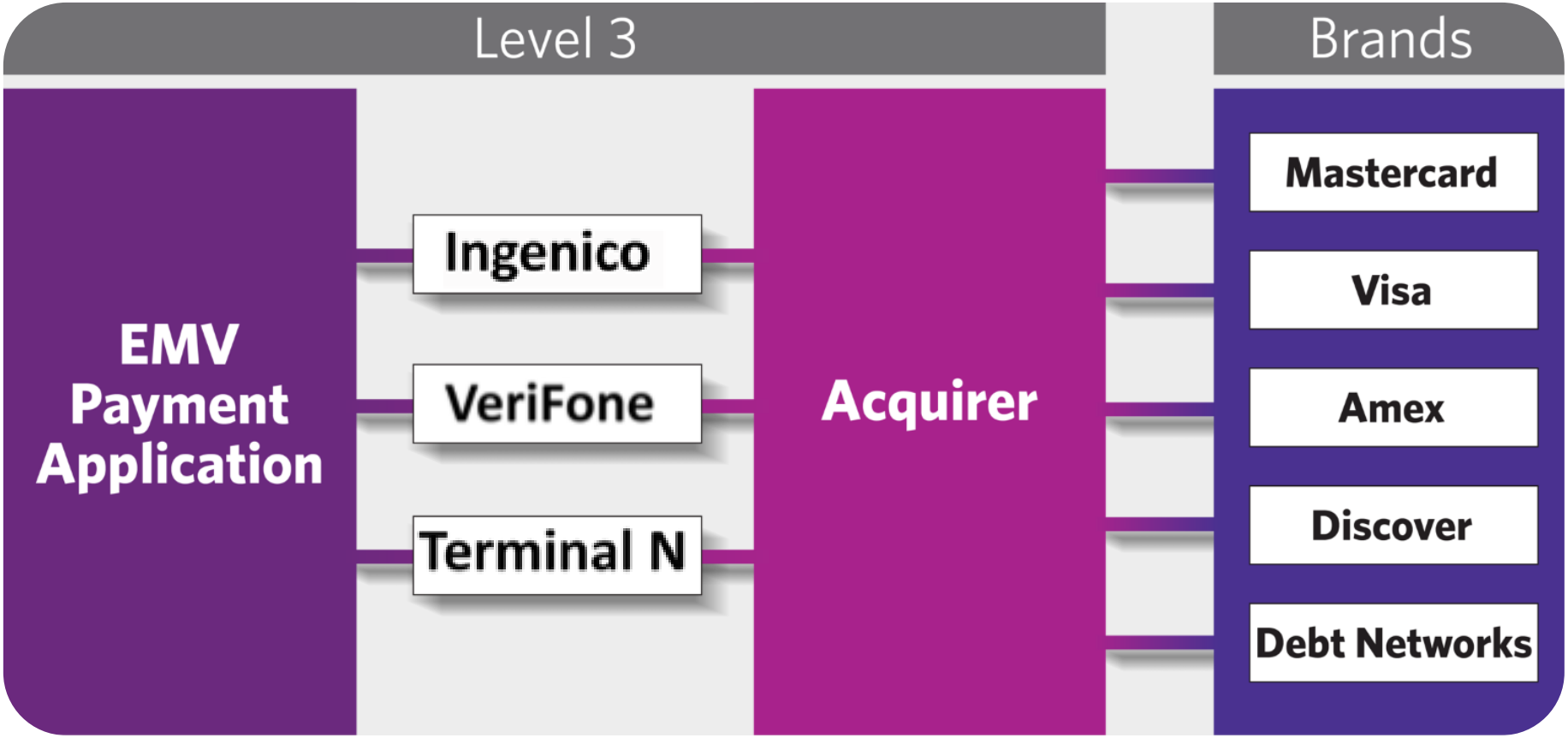
EMV Levels

1	Contact chip reader in PINpad terminal	*Letter of Acceptance* lasts 4 years
2	EMV Kernel in PINpad terminal	*Letter of Acceptance* lasts 3 years
3	EMV Payment Application accessing EMV Kernel	*Letter of Acceptance* lasts 3 years

EMV Level 1 & 2



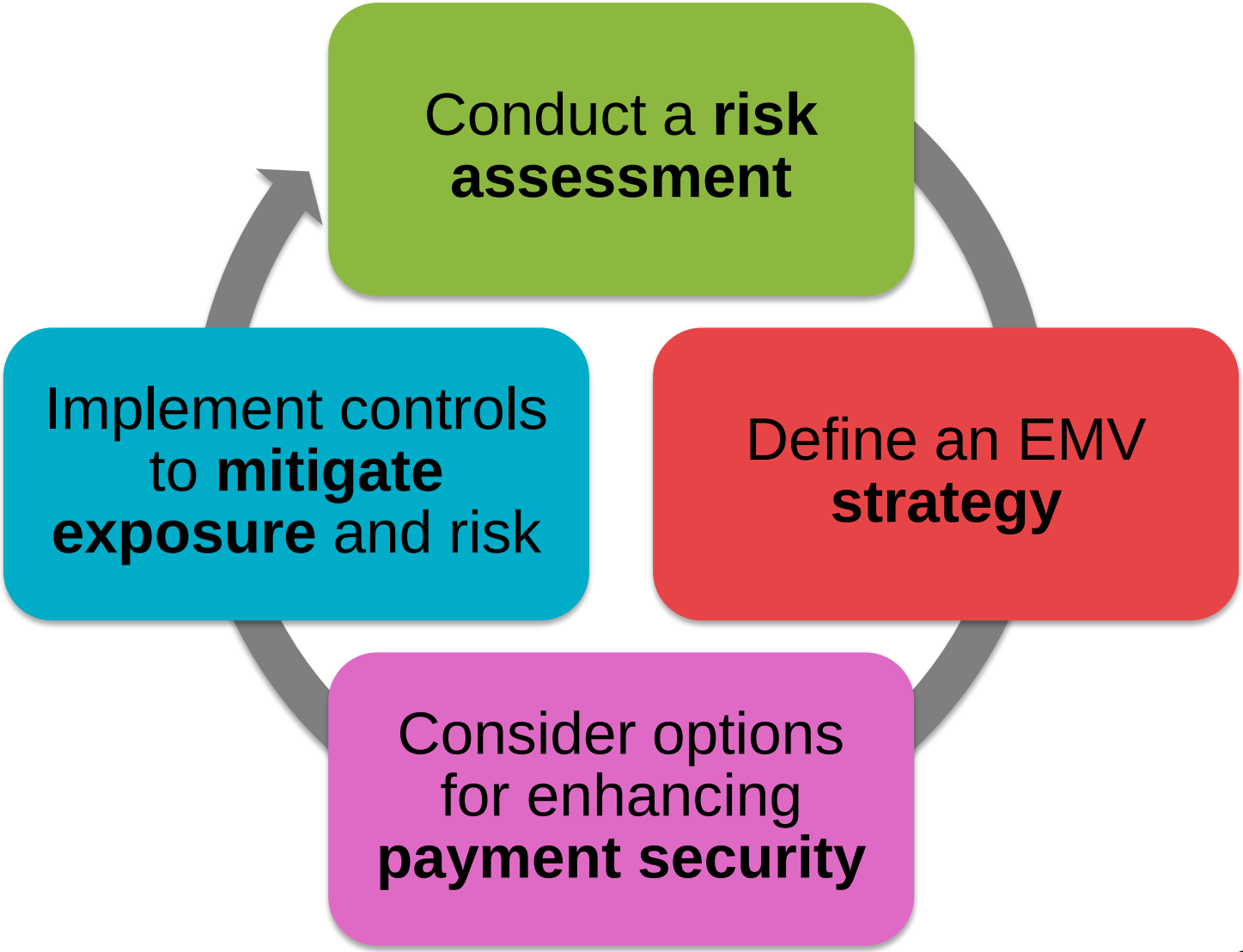
EMV Level 3



EMV Level 3 - Development and Certification

- Entire **transaction flow** is required for Certification
- **Certification** required for each Card Scheme
- Certification **Expenses** (subject to change)
- EMV can add an **additional 120-180 days** for new integrations or Certifications

EMV: What You Can Do RIGHT NOW!



EMV: Alone is Not Enough

- **Remain Vigilant – Criminals shift and evolve their tactics**

LAYERED SECURITY APPROACH

How Can We Protect Payment Data?

EMV

Encryption

Tokenization

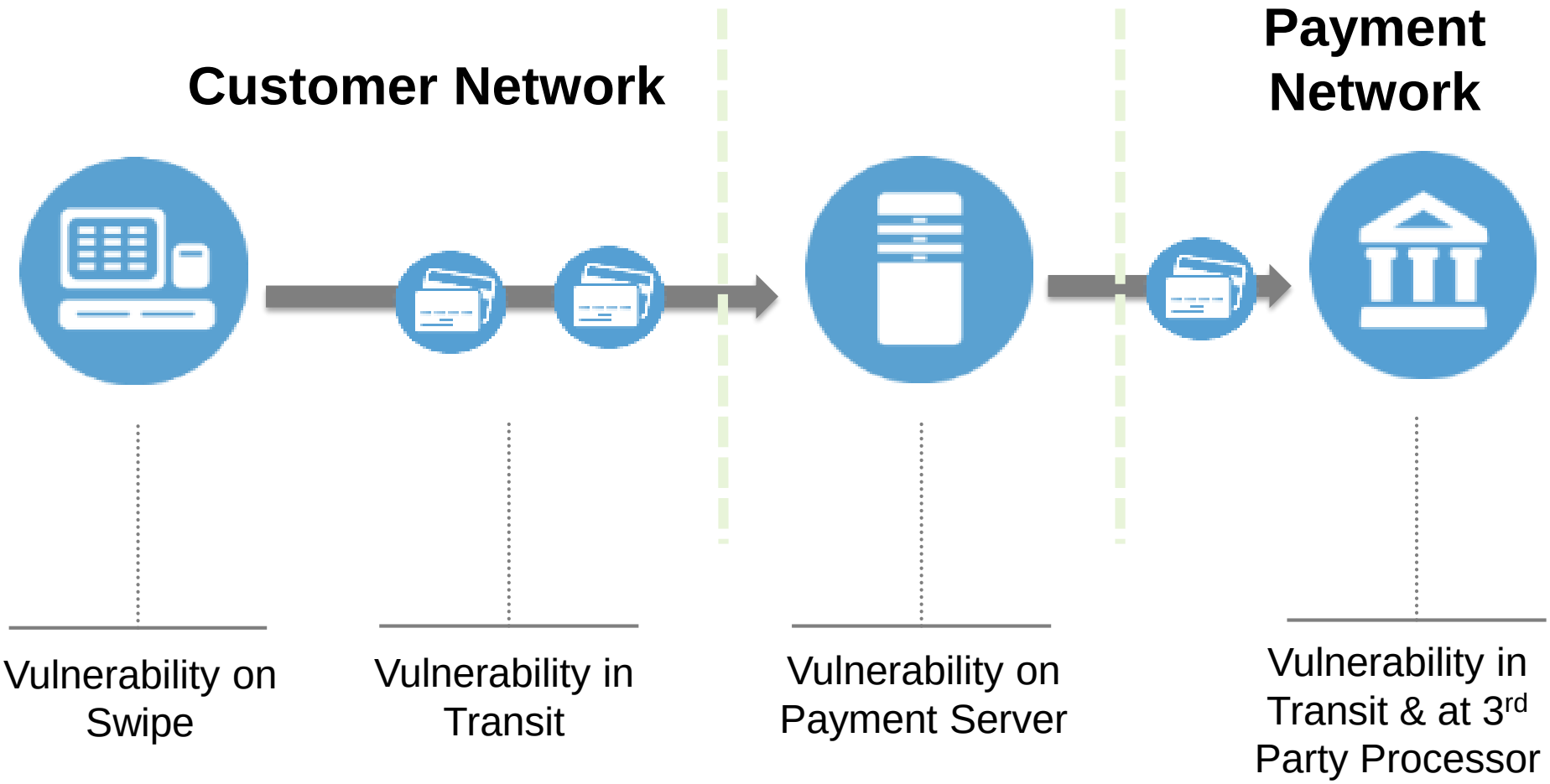
PCI DSS Compliance

Your Security Foundation

The toolbox must be accompanied by business practices and processes designed to reduce exposure and control risk.

Elavon

Vulnerabilities



STEPS TO EMV READINESS

Elavon

EMV Strategy Planning

Perform a security assessment

- Identify vulnerabilities
- Layered approach to security
- Identify other payment update opportunities

Find a provider

- Project Management & technical support
- Solid experience & long-term plan

Prepare Your Business

- Define project and budget resources
- Set expectations
- Train employees and inform customers

Maximize Your Effort

1. Security

- ✓ Eliminate storing card holder data within your environment

2. Reduce PCI Compliance Burdens

- ✓ Reduce PCI exposure from POS/PMS
- ✓ Reduce time and effort expended on PCI compliance

3. Future Proof and Liability Shift

- ✓ Seek a solution that is EMV, contactless and mobile ready

4. Reduce Vendor and Payment Complexity

- ✓ Seek a solution that fits your POS/PMS Vendor
- ✓ Remote updates and management of payment application

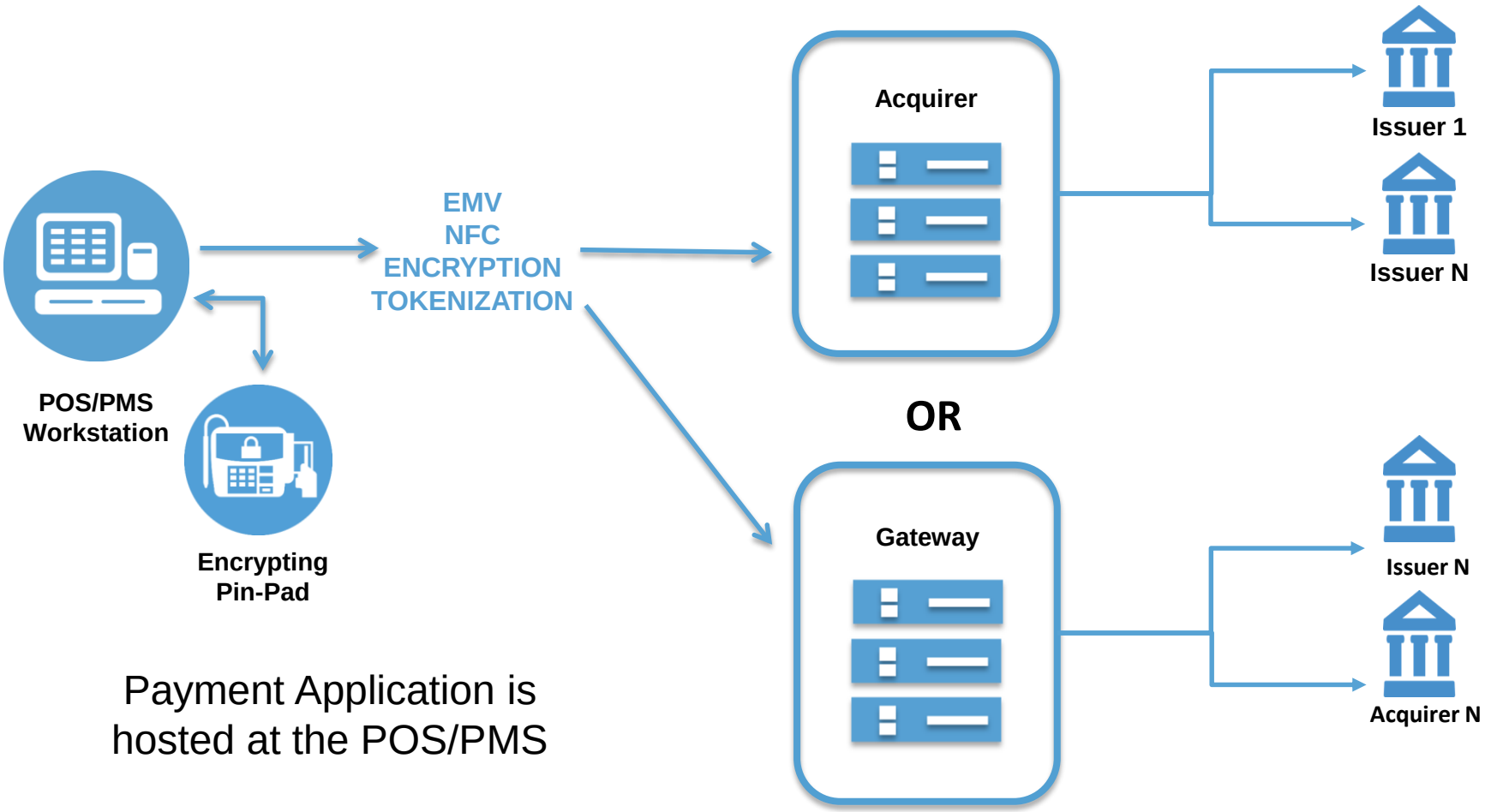
INTEGRATION OPTIONS AND AVAILABLE SOLUTIONS

Elavon

Solution Models

Solutions	Who performs the work?	Future proofing
Fully Integrated	Merchant or POS/PMS Vendor	High degree of difficulty for developer
Stand alone terminals	Terminal provider (usually Acquirer)	Subject to Terminal provider resources
Semi-integrated	Shared with the Payment Application provider	Development responsibility can be shifted to Application provider

Fully Integrated Solution

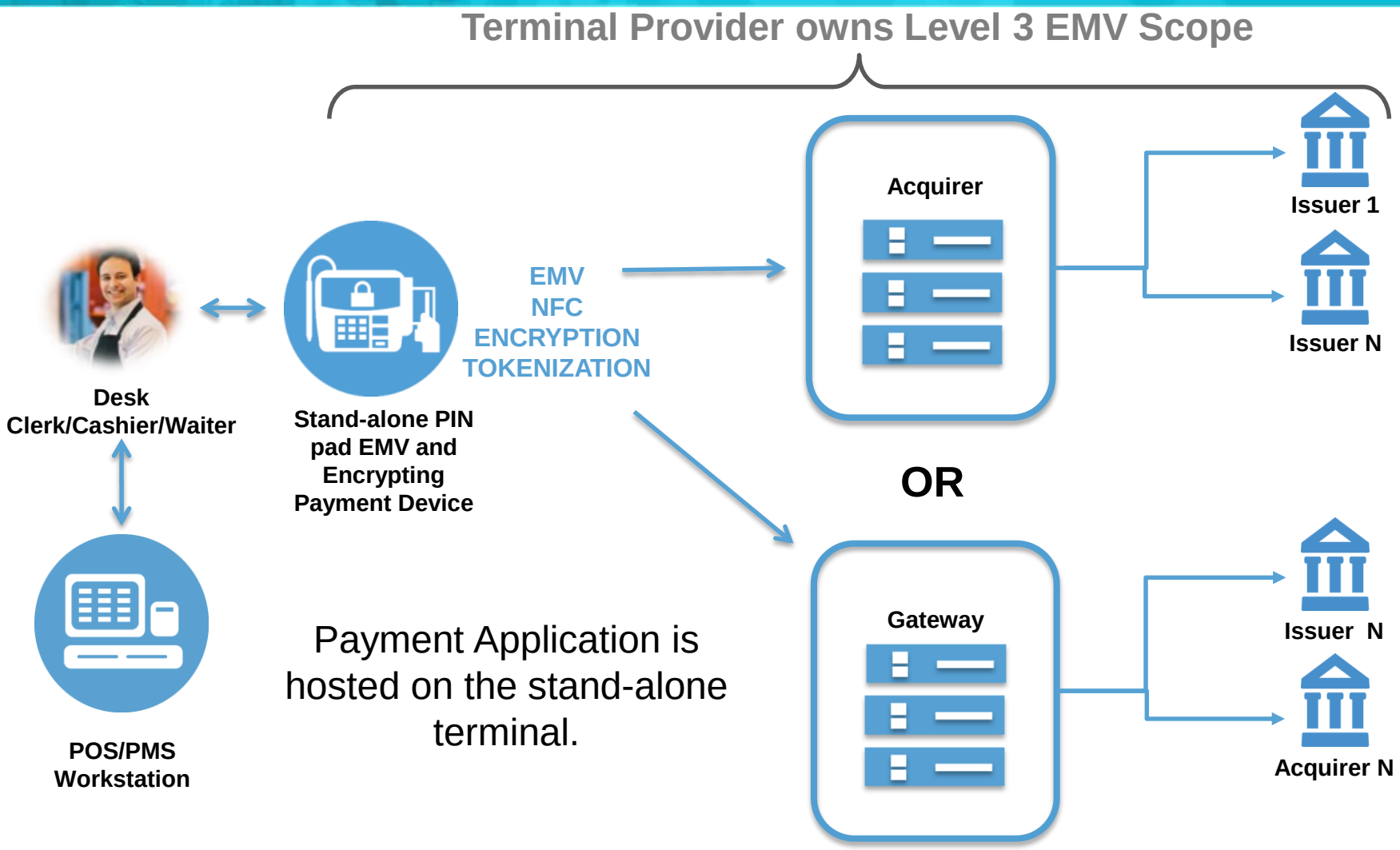


Payment Application is hosted at the POS/PMS

Merchant, Vendor manages Complex, Level 3 EMV Scope

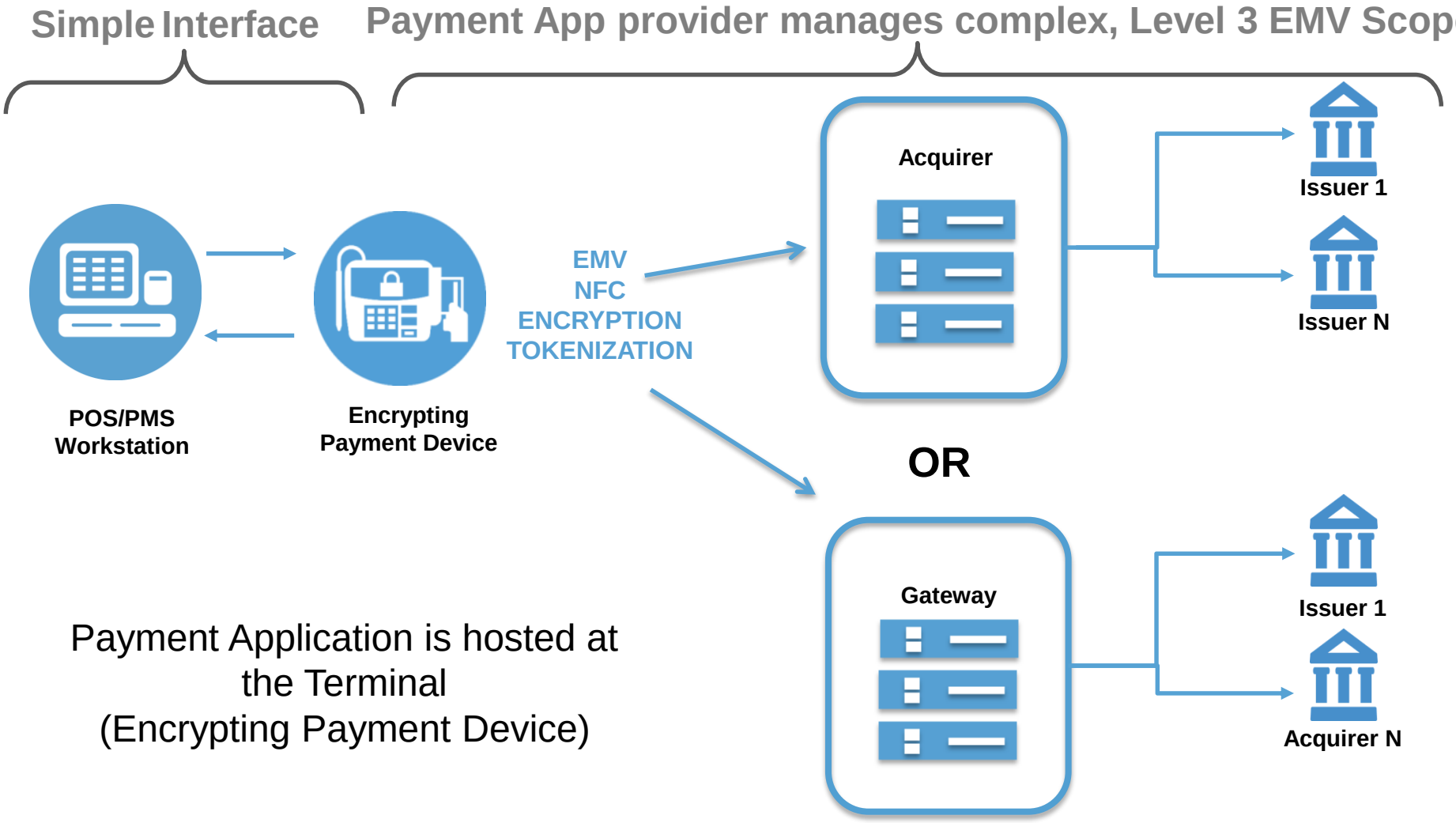
Elavon

Stand-Alone Terminal Solution



Elavon

Semi-Integrated Solution



Payment Application is hosted at the Terminal (Encrypting Payment Device)

Elavon

Which Solution Fits Your Business?

Solutions	Ease of Use	Maintenance / Ownership
Fully Integrated	Generally Easy, if designed to Merchant requirements	Significant effort on Merchant (POS/PMS Vendor)
Stand alone	Requires dual entry of all credit card payments accepted	Minimal effort on Merchant; falls to Terminal provider
Semi-integrated	Generally Easy, retains single transaction entry to system	Moderate effort on Merchant, Vendor, Shared

THANK YOU

for attending today's presentation!

If you have any questions please email presentations@Elavon.com

Elavon